Evolving Interoperable Network Architectures for NATO Coalition Forces

Barry Sowerbutts, Richard Sharman, Mark West
Roke Manor Research Ltd
Roke Manor, ROMSEY
Hants SO51 0ZN
UK

barry.sowerbutts@roke.co.uk

ABSTRACT

Military communications capabilities have evolved under stringent requirements for reliability and security. Today, these legacy systems need to support Network Enabled Capabilities (NEC) but are challenged to provide the bandwidth and interoperability common in civilian systems. Internet Protocol (IP) has become the universal standard for flexible networking and the pre-requisite for advanced solutions. Consequently, a network architecture for NATO coalition interoperability must integrate the legacy and IP worlds. Various factors, such as security, subnetworking, information management and mobility management for NATO requirements are examined in this light and a proposal made for a generic Defence Intranet Architecture (DIA) framework from Commercial-off-the-shelf (COTS) components. The architecture supports future C4ISTAR requirements and a battlefield communications subsystem (BATCOM) is shown as an example of the architecture. The relationship of the architecture to NATO INSC is discussed and the work undertaken by RMR to address one of the issues is summarised. Also the relationship with the EU project MIND is discussed in the context of trust in coalition networks. The increasing commonality of modern military and civilian communications requirements demonstrates the need for converged architecture frameworks and dual-use product offerings.

Keywords: NEC, COTS, IP, INSC, C4ISTAR, MIND

1.0 INTRODUCTION

Battlefield communications have been driven historically by requirements for highly-robust, highly-secure, bespoke systems usually designed and procured for a single purpose. These systems implement high performance solutions at the expense of adaptability and interoperability. For example, Ptarmigan (Tactical theatre telephony backbone system) carefully matched bandwidth, bearer technology, security and other factors to voice telephony needs.

Proposed UK military communications systems such as Falcon, Cormorant and Bowman provide new functions and increased bandwidth by exploiting Internet technologies on the inside, but typically do not exhibit externally the architectural flexibility to allow full interoperability and extendibility. Moreover bespoke systems are typified by long procurement cycles leading to potential mismatches between delivered system performance and perceived requirement at the time of delivery.

In the mean time, the civil communications has experienced a revolution in information availability enabled by the Internet Protocol (IP). The commercial world has converged on IP architecture-based solutions in timescales which rapidly outstrip military procurement cycles. This convergence has provided a high degree of application sharing and extensibility while transparently exploiting diverse underlying communications technologies and resulting infrastructures.

Paper presented at the RTO IST Symposium on "Coalition C4ISR Architectures and Information Exchange Capabilities", held in The Hague, The Netherlands, 27-28 September 2004, and published in RTO-MP-IST-042.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
01 DEC 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Evolving Interoperable Network Architectures for NATO Coalition Forces	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Roke Manor Research Ltd Roke Manor, ROMSEY Hants SO51 0ZN UK**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADM202135, RTO-MP-IST-042. Coalition C4ISR Architectures and Information Exchange Capabilities (Les architectures C4ISR et les capacites d'echange d'information en coalition)., The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**32**	

The advanced concepts of NATO INSC [8] and the network-centric vision of the US Network Centric Warfare (NCW) [1] or UK Network Enabled Capability (NEC) [2] will enable flexible and rapid force deployment. But these developments are predicated on capacity and interoperability requirements and call for the investigation of advanced network architectures to address these issues [4]. Advanced techniques for IP traffic performance enhancement, such as robust header compression [5], session enhancement [6], and mobility [7] are needed to address challenges in both military and civilian domains.

1.1 The Problem – Getting From Here

Emerging systems will extend, and eventually replace, current systems, but factors such as procurement, training and deployment costs mean that legacy systems will continue to play a role for a considerable time. Operational needs will require rapid evolution to support new capabilities and to improve performance. Procurement priorities, and policy changes for tactical or strategic needs, may cause tensions as coalition partners move at different rates.

Since legacy systems are usually optimised for single service delivery over bandwidth-limited bearers with closed-interoperability demands, it follows that flexible service delivery on available carriers will not be achievable by simply layering additional function over legacy communications bearers. Instead, the capacity required will be achieved by providing additional bandwidth over new bearers. Satellite services, digital audio and video broadcasting, wireless LAN and Ultra Wide band (UWB) are examples of existing or possible systems. Such is the intensity and ingenuity of effort in the commercial world that solutions to capacity requirements will most probably be overcome in the post-Bowman time-frame.

Interoperability will, however, remain a persistent problem for the foreseeable future. High bandwidth links may be expensive and the need to reuse and reconfigure them will lead inevitably to Internet-like use patterns. Multiple, independent services will be are layered over common transmission media, regulated by quality of service objectives. Obtaining capacity where and when necessary, from in-house or commercial operators, and exchanging information with coalition partners, will be the factors driving the structure and layout of future communications systems.

Of course IP adoption alone does not bring universal interoperability, but it does enable security, scalability, quality of service (QoS), and many other issues to be systematically addressed. It forms the de facto starting point for any modern network architecture solution. IP is, itself, evolving to address both commercial and military requirements.

1.2 Assumptions - What we can guess about the future

Technology mediated change does not come free, and will alter the balance of investments in the lifecycle. Generally speaking the trend in modern communications is towards decreasing costs at the operational stage while increasing costs in the earlier stages of the development cycle.

COTS equipment is usually engineered to be good-enough-for-purpose and may not immediate satisfy military requirements. However, no technology can be totally reliable, or secure, so even networks specifically procured specifically to achieve these aims, often fail to fully meet their objectives.

Paradoxically however, it is possible to build reliable end-to-end communication on an unreliable bearer (by techniques such as packetisation, selective retry and spread spectrum coding). It is, similarly, possible to build secure end-to-end communication on insecure links (by using cryptography, steganography, and other approaches). Consequently, COTS networking, with its attention to quality of service, best achievable effort, and cost-effective bandwidth utilisation is a good place to start when designing a mission critical communications service. Anti-jamming, anti-spoofing, privacy protection, authentication support, reliable delivery and other characteristics can be added as and when needed, according to costs and benefits.

Where military-specific functionality is not supported by COTS equipment, additional functionality needs to be added in a future-proof way to avoid obsolescence and enable product enhancement. This again strongly predicates an Internet-like development effort where incremental function can be architected as needs arise, in ways that do not conflict with fundamental principles [3].

1.3 Some Critical Constraints

The critical topics which constrain communications network architecture can be summarised as follows:

- Command and Control function (C2) implies the need for low bandwidth, low latency, high security communications. This need is satisfied today by bespoke systems, and will continue to be a requirement. However they may need to be increasingly flexible in the context of rapid reaction forces, asymmetric threats, peacekeeping missions and coalition activities.
- Increased information dissemination and sharing (ISTAR) at all levels in the military command hierarchy implies need for high-bandwidth communications systems with adjustable latency, and flexible security. This requirement is not easily available within current military capabilities, but is well satisfied by existing commercial world capabilities.
- Addressing, Routing, Discovery, and Configuration needs in military deployed systems will stress the capability of military equipment in terms of flexibility. However, these are also commercial imperatives, and partially available solutions exist today.
- Flow control, quality of service, network management, and capacity acquisition in the military domain implies the need for a more cost-sensitive, service-acquisition, approach to communications system provision. This is strongly developed in the commercial world and already emerging in military systems.
- Application innovation in the military domain will accelerate, implying need for application interface transparency.
- Security policy will remain an important aspect of military communications, but with a broader meaning, encompassing denial of service, as well as the more traditional privacy protection and authentication control.

2.0 A DEFENCE INTRANET ARCHITECTURE

The solution to network implementation uncertainty is to plan, from the beginning, for a world in which bearer technologies change, networking protocols and standards evolve, and applications change according to operational need. In this respect ISTAR capabilities and C2 applications can be seen as flexible services which must be supported by available infrastructures. However, given the specific requirements of C2 systems and the considerable investment in legacy and future legacy systems a pragmatic approach to achieving interoperable network architectures is to retain the best parts of legacy C2 systems, while building interoperability interfaces to new function implemented on Internet-based architectures.

The INSC programme [8] simulated a coalition IP network. The aim of the Defence Intranet Architecture is to evolve INSC concepts to allow the creation of parallel universes of multiple networks, interconnected by gateways using Internet standards. The result is a closed intranet implementation displaying multiple security and function levels which can be built on COTS components, and which allows different subnets to evolve at different rates according to need.

This section presents the core concepts of the architecture and then describes the principles of the network architecture. The section then discusses how the architecture can be extended to support coalition operations. Some thoughts are given on how to create a DIA compliant network and a case study is provided by way of an example.

2.1 Core Concepts of the Architecture

The core concepts of the proposed architecture are to define legacy systems as mission critical C2 towers with defined entry points. New function is implemented as enterprise networks with defined interoperability mediated by firewall and router policies. A network of networks, connected by gateways, NAT boxes, and proxies implements various aspects of network management as needed. Applications can run in a number of modes, but typically using the web application metaphor, employing HTML, XML, applets, and other functional devices.

Figure 1 shows the Defence Intranet Architecture (DIA) concept, which links legacy C2 systems (shown as a pyramid) to local ISTAR Intranets (accessed by portals) and which was originally generated in response the UK MOD NEC initiative.

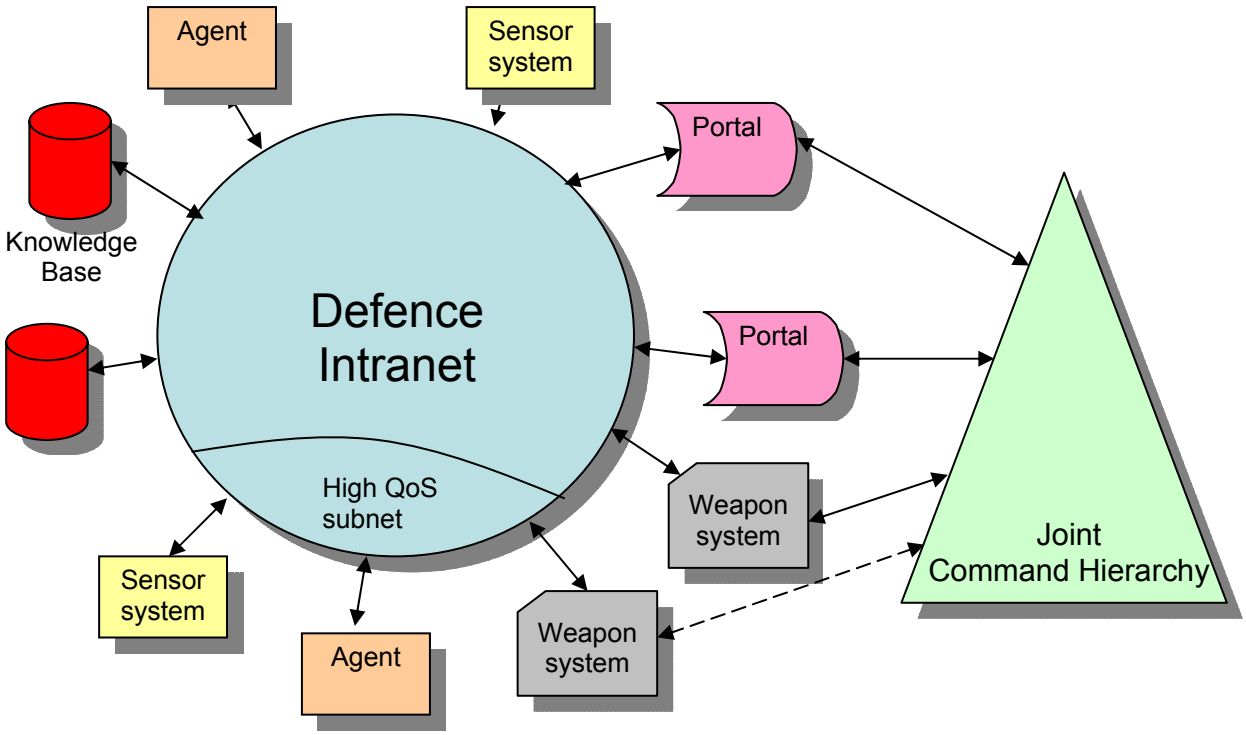


Figure 1: The Defence Intranet Concept in its General Form.

The key feature of this architecture is that it permits mission critical C2 decisions to be made, within a distributed sensor-to-shooter framework, using a highly robust and secure communications environment. Bandwidth-hungry accumulation of valuable information from dense information spaces can be achieved in a COTS-enabled infrastructure. Hardened as appropriate, this infrastructure can inform military decision-making using a flexible, seamless access to emerging ISTAR assets. The elements of the architecture are as follows:

- Joint Command Hierarchy communications – The joint force command and control chain which establishes high availability, high mobility connectivity between force components.
- Defence Intranet – which provides connectivity and information sharing between sensors, shooters and information processors. The defence intranet will also have High Quality of Service Subnets where time-critical sensor-to-shooter links are required.
- Weapon Systems – the military hardware - which can be targeted and/or released via the intranet using web-based management tools or from command elements.

- Sensor Systems – which are targeted via the intranet and which may include both traditional sensors e.g. SAR as well as innovative COTS offerings including web-cams on expendable UAVs.
- Knowledge bases – which are repositories of information gathered from a multiplicity of sensors, possibility processed by software agents.
- Portals – which provide an information-filtered gateway between the defence intranet and force elements. Gateways between networks will be particularly important as these are points of control for the filtering and translation of data between networks.
- Agents – software technology which intelligently processes information available on the defence intranet, working autonomously and cooperatively to aid ISTAR analysts, and can also alert force elements or weapon systems.

2.2 Principles of the Architecture

The network architecture conforms to the following principles:

- A network element should be autonomous, and self identifying. Network elements should be a generic computing system able to support a communications sub layer as well as an application environment layer. In the case of an ultra small element (intelligent munitions, sensor post, etc.), this may be implemented as a single chip with read only (flash) memory. In the case of larger node (vehicle control, headquarters function, etc.) this may be one or more computational platforms in local area networks with embedded routers, servers, user interfaces, and other functions.
- A network is formed by linking network elements with one or more communications subsystems. The linking and unlinking should be transparent to the application (although the effects might be evident to an end-user at the network element because of loss of service). Elements in a network should discover their neighbours (as in IPv6).
- A network of networks is formed by linking networks together. Every network has the capability (potentially) to act as a router of messages between other networks. The degree to which this happens depends on bandwidth and demand.
- A universal addressing policy allows any end users to communicate. Military networks have a unique need for multicast transmission, as well as the more normal unicast transmission. Headquarters commands to all brigades, brigade command to all units, etc. are examples of obvious multi-cast applications. Sensor input to multiple users (intelligence, command post, NGOs, news media, are other examples of potential multicast applications).
- Network layering is universal, and transparent to end users. The tight link between bearer technology and application should be broken. A voice stream is merely a real time bit stream at a voice data rate. It should not matter whether the bit stream is carried over a radio link, a wired link, or a satellite link (as in fact happens in the commercial telecommunications world). The layers which all elements should support are:

  a) Communication bearer, e.g. CNR, GSM, ATM, etc.

  b) Communication Protocol, e.g. IP

  c) Application supported over Military Application interface, e.g. NBC BISA

  d) User interface, e.g. graphical user interface with windows.

It will be observed that the principles given here are satisfied by IP in its most general form (and perhaps other network systems). Fundamentally – by separating bearer from application following Internet-based principles the architecture support rapid incremental evolution of capability.

2.3 An Extension to the Architecture to Support Coalition Operations

Interoperability has always been a significant challenge for NATO alliances with interoperability achieved primarily through procuring standards-compliant systems e.g. Link 16, which have highly specialised functionality or through expensive bespoke gateways. In contrast, this Defence Intranet Architecture provides a vital and simplifying interoperability mechanism for coalition communications, where all partners gateway to a common Intranet. This requires N gateway designs for N partners, rather than the N2 interfaces which would otherwise be needed.

A generalisation of the Defence Intranet Architecture is shown in Figure 2 where several distinct intranets and command hierarchies, possibly in different coalition force groups, are connected by Internet backbones (shown as a central network cloud) creating a multi-security, multi-layered C4ISTAR network built primarily on COTS technologies.

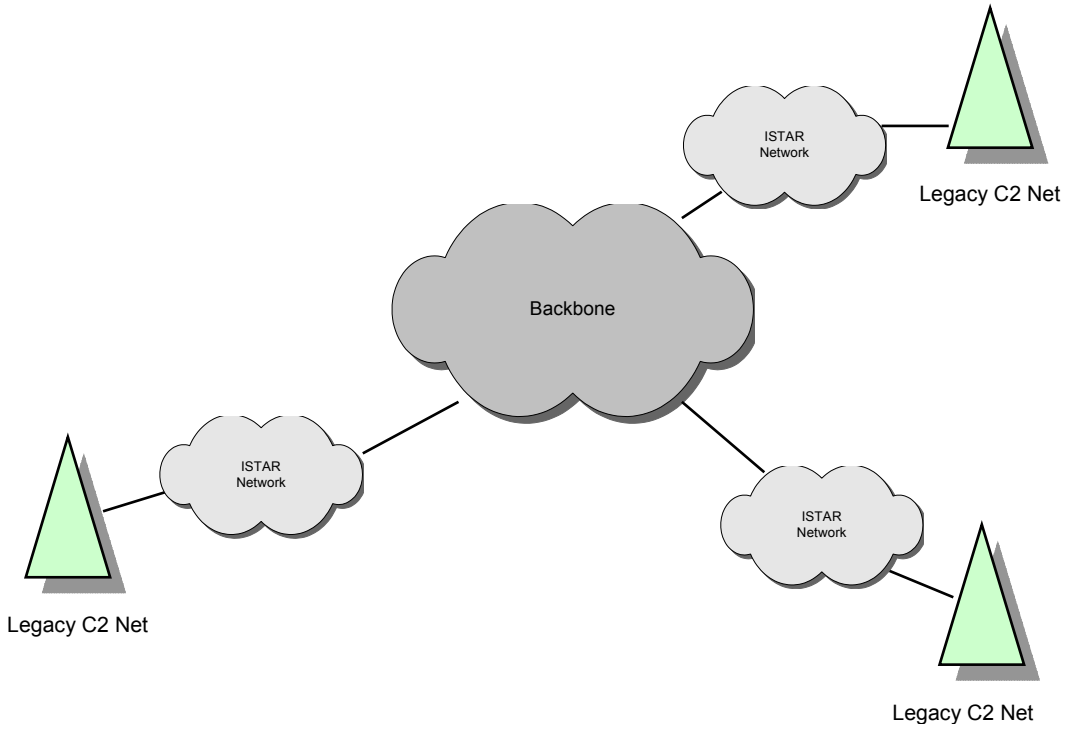


Figure 2: Defence Intranet Concept for Coalition Operations.

2.4 Creating a DIA Compliant Network

The steps to creating a DIA compliant system include:

- Address space definition: the selection and standardisation of IP address spaces, associated domain names, neighbour discovery, autoconfiguration modes, choosing IPv4 or IPv6 as appropriate.
- Routing policy selection: the establishment of routing policies which enable adaptive routing, quality of service provision, and mobility support. Of particular interest are the use of tunnelling mechanisms for VPNs.
- Management policy selection: the use of ad-hoc, remote and automated management approaches to enable military networks to be configured rapidly, deployed quickly, and adapt to battlefield requirements.

- Legacy interconnection: where appropriate, legacy systems need to be attached by bridges, firewalls, NAT boxes and human interfaces.
- Application growth enablement: evolving requirements, novel sensor and data mining technology, and the need to re-use capability according to mission argue strongly for all future systems to be designed as general purpose, robust and adaptable as possible.

2.5 Novel Application Enabling

Conventional applications for network support are command and control (primarily sending messages out from headquarters to active units), and intelligence-gathering (primarily sending raw data in to data fusion centres, such as Battlefield Information System Applications - BISAs).

Some examples of novel applications which require more innovative network solutions are:

- **Location dependent services**. In future applications (and planned for the US FCS) is the capability for every soldier, vehicle, unit, etc. to be able to know where it is in the world, using GPS. It will also be possible to relay this information to others. Provided the individual soldier, force element is also identified (in terms of name, capabilities, etc.) it will be possible to determine the needs and capabilities of all elements.
- **Sensor-to-shooter connection**. In legacy systems either the sensor is closely related to the shooter (e.g. gun sight and gun control) or it is remote (order of day to bomb at Lat/Long from B52). In modern warfare there is a requirement to link the sensor and shooter much more closely (UAV camera locates terrorist, ground force engages terrorist, satellite performs battle damage assessment, etc.).
- **Gateway filtering, intercept**. Gateways between networks will be particularly important as these are points of control for the filtering and translation of data between networks. Gateways may operate agent technologies to determine the capabilities of networks, as well as to perform Data Fusion functions such as data visualisation, data interpretation, command modelling, etc.

3.0 A CASE STUDY ON BATCOM – MILITARY USE OF CIVIL INFORMATION MANAGEMENT TECHNOLOGY

A common requirement in platoon-level communication is to implement a real-time, all-informed, voice message interchange environment as a battlefield communication system (BATCOM). This has conventionally been satisfied by an analogue, broadcast, voice radio solution such as Clansman. In the modern digital world the concept becomes a near real-time, peer-to-peer, audio-visual environment system, satisfied by PC laptop processing, webcam data capture, electronic whiteboarding, GPS positioning and ad hoc networking exchange, as indicated in Figure 3.

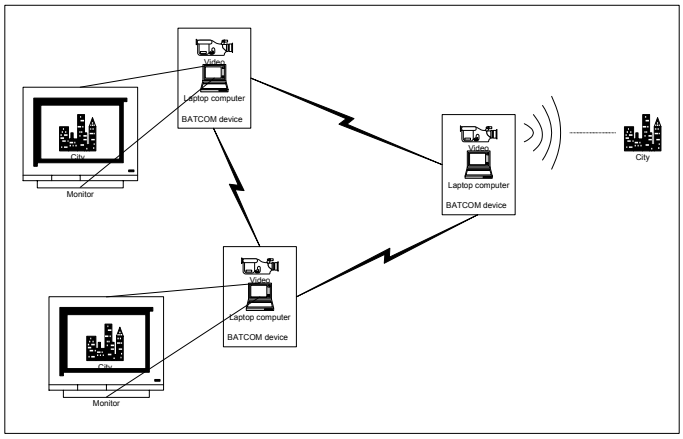


Figure 3: Physical Architecture of BATCOM ad hoc Network System.

The physical arrangement can be implemented in a number of ways, but a typical approach is to model true peering by client-server mirroring as shown in Figure 4. This has the advantage of scalability, and enables application sharing, and distributed data base functions, without the need for traditional high function servers and other internet support, which might not be available in the battlefield.

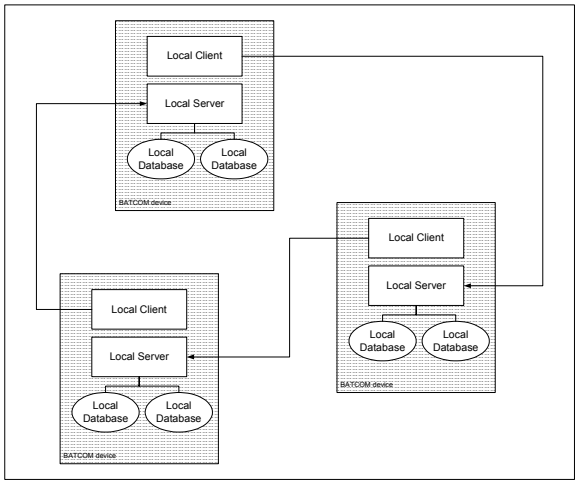


Figure 4: Logical Architecture of BATCOM ad hoc Network System.

A typical test configuration uses a small-scale wireless ad-hoc network between laptop PCs to demonstrate an autonomous ad-hoc network, utilising IEEE 802.11 WLAN technology. The system is potentially extendable to any size network (using concepts developed in MIND [12], creating a dynamic, self-deploying and self-healing shared audio-visual environment.

4.0 ISSUES

4.1 IP Interoperability

Although the ubiquity of IP is one of its great merits, the potential migration from IPv4 to IPv6 may have a significant impact on interoperability in the future. This has been a subject of considerable attention in the IETF and solutions have been proposed - including tunnelling. In the INSC programme, which

comprised multiple subnets with mixed v4/v6 pedigree, one of the consequences of the architecture was the existence of multiply-tunnelled IP packets with concatenated headers. Added to this, many of the tunnels were IPSEC encrypted and the resulting packet headers in many cases were substantial, sufficient to risk exceeding the MTU limit for some media, and more generally potentially adding significant overhead over wireless communications links.

As its contribution to the INSC programme RMR provided novel robust header compression software integrated with the IPSEC gateways which substantially reduced header overheads in the network. The following illustrates, in graphical form, the impact of header compression on the various protocol stacks that were encountered in some of the tests:

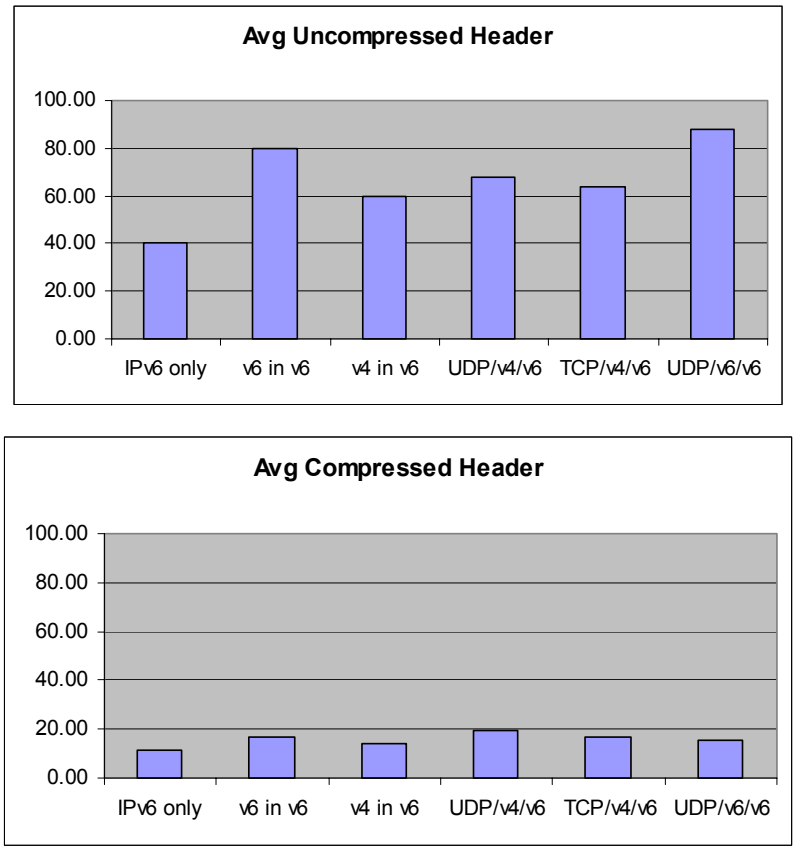


Figure 5: Header Compression Performance.

The following graph shows the distribution of packet losses (as burst losses) across a variety of tests in the network. Despite these losses (up to 15 packets in a burst), the EPIC header compression caused no additional packet losses. This demonstrates the reliability of the header compression techniques.

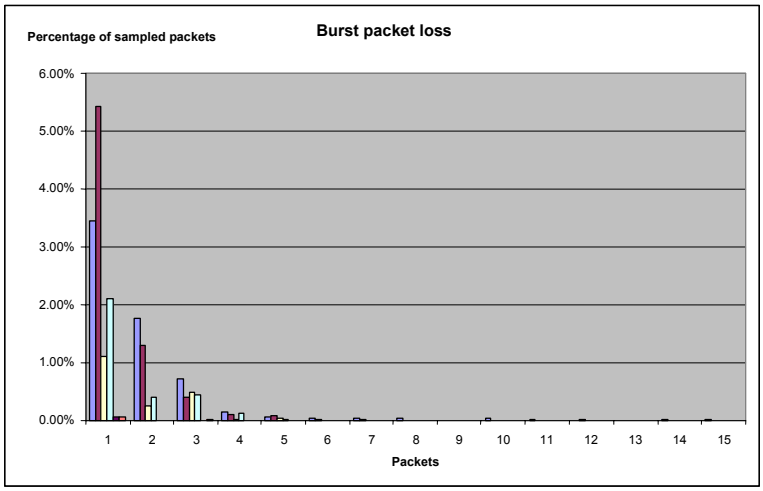


Figure 6: Packet Loss Observed.

4.2 Trust and the Coalition Network

The proposed Defence Intranet Architecture, wherein alliance partners have access to a shared set of resources, brings many advantages in terms of collective decision-making but raises issues in the respect of trust. For example consider the case of a UAV owned by one partner which may need to use the resources of several other partners in order to make its sensor information available to all.

The issue of trust in open IP networks has been a subject of investigation within the EU IST 5th Framework project MIND [12]. Within this programme has studied the evolution of IP access technology for Mobile IP-based Network Developments. MIND assumed that a mobile node might connect via a number of hops across other mobile nodes forming ad-hoc network clouds at the edge.

- The MIND framework, as shown in Figure 6 employs the following concepts:
- **Domain Boundary Establishment**: a node can identify other nodes within a boundary of mutual trust. A node can trust a group of peers (e.g. same regiment) or have a different relationships (e.g. with headquarters)
- **Intra-Domain Mobility and QoS**: groups of nodes share a common mobility and QoS model, within a given domain. No ad-hoc networking protocol will suit every need, but current MANET protocols are good enough, and current QoS models, such as diffserv, are adequate for a range of needs.
- **Peering**: there must be ways domains to connect. Existing routing protocols (e.g. OSPF and BGP) can peer, but probably not comprehensively enough.
- **Network Join and Leave Negotiation**: when a device attaches there needs to be a negotiation on appropriate mobility mechanisms. This negotiation is carried out within a trust relationship established by domain boundary establishment.
- **Interdomain Context Management**: a node may wish to request non-default QoS for its packets across multiple domains. The extent to which state can be created also becomes a question of trust relationships.
- **Dynamic Reconfigurability**: Join negotiation may fail because a device does not support the appropriate protocol. However, with the right constraints and trust-models, reduced functionality can be achieved.

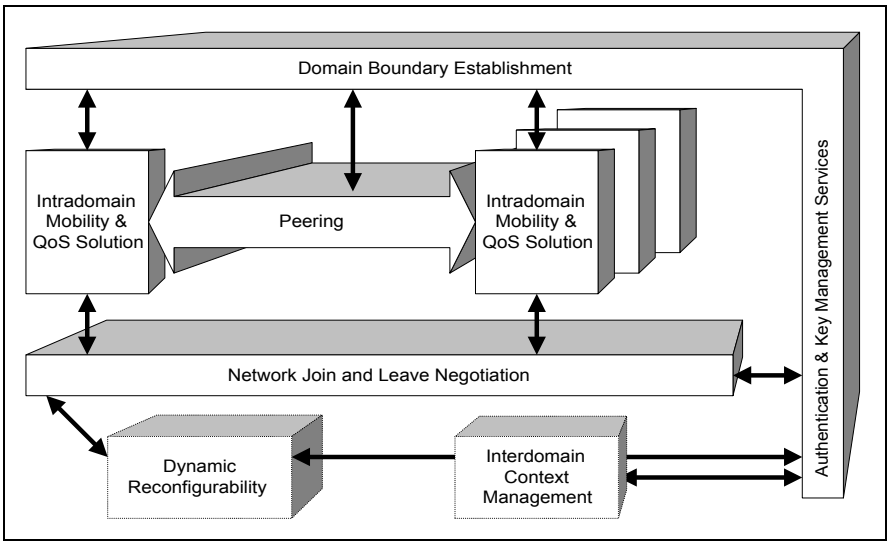


Figure 7: Trust Boundaries in MIND.

The concept of ad-hoc clouds of nodes connecting to another network is a powerful metaphor provided nodes can establish trust relationships with the network. This can be achieved by AAA protocols such as EAP (Extensible Authentication Protocol) or RADIUS (Remote Authentication Dial-In User Services); or security protocols (IPsec, or HIP – the Host Identity Payload).

The concept of a tunnel has proved very fruitful for implementing a range of QoS and Security capabilities. For example, a tunnel can support a secure connection across an arbitrary cloud of untrusted nodes, and a cloud of nodes with mutual trust can decide to allow untrusted connections to transit the network, encapsulated in a secure tunnel.

This work clearly has its origins in the civil domain but as civil and military requirements converge the model may have increasing relevance to the proposed Defence Intranet Architecture.

4.3 Risks in Using Commercial-Based Architectures in Military Systems

The key risks in introducing a commercially-based intranet architecture into military usage are:

- The unknown factors inherent in the approach which may lead to vulnerabilities in deployed systems. This is always a risk with system architectures, but arguably building from an IP base is more risk averse than almost any other approach.
- Perpetuating vulnerabilities in military systems which are consequent on design decisions valid only in the commercial world. In commercial terms secure privacy is possibly less highly valued, but authenticity more highly valued, than in the military world. However, the convergence of commercial and military value systems, and the consequent increase in dual use technologies makes judgements such as these less useful. What is important in one domain is also important in the other.
- Successful deployments will be vulnerable to obsolescence. This is a major concern in bespoke system, and conversely less of a concern in an open architecture.

4.4 Implications of an Intranet-based Approach

The C4ISTAR implications of the architecture proposed are that robustness and security become adjustable factors, capable of being engineered according to need. The intention is to enable seamless

access to legacy and emerging applications. At all stages the requirements of robustness, migration, and implementation cost can be adjusted to suit objectives and budgets.

The commercial implications are that, since the COTS approach to component selection is assumed, the case for hardware and software acquisition, system management tools selection, operation policy, purchasing strategy, de-commissioning approach, replacement strategy and many other issues become amenable to current commercial best practice.

The security implications are that threat analysis, virus resistance, counter attack strategies, and mediation of vulnerabilities become amenable to evolving methodologies from commercial practice. Since most security exposures are not achieved by cracking cryptographic codes, but by subverting the social environment in some way, it follows that a whole-system approach to security is needed, rather than an "accrediting crypto" approach [11].

4.5 Implications for Procurement Strategy

Military networking procurement is moving from a philosophy of cyclical replacement to one of continuous replacement based on currently emerging COTS technologies. The disadvantages of current procurement strategies are that they lead to unique, stovepipe, non-interoperable solutions which are locally optimal at best. Separate solutions are usually necessary for network-wide functions such as security. A lack of attention to system maintainability, installability and interoperability is characteristic, and overall military budget costs are not minimised.

Specific procurements are valid where unique factors apply (such as operation in extreme environment conditions, at unusual range, or subject to specific enemy threats e.g. jamming). Bowman may be an example of this.

Generic procurement principles should be employed for most of the defence Intranet architecture based on COTS technologies and commercial state-of the art network design. Such networks can be augmented with function over time to satisfy specific shortcomings with respect to military requirements. An NBC sensor network could be an example of a new network designed to new requirements but implemented in such a way.

5.0 CONCLUSIONS

Architecture frameworks have proved useful to advance the design of robust, interoperable and secure networks. Since commercial developments have proceeded faster and further, and since a wide range of cost-effective products is available, it is logical to start from a COTS-based position.

The advantages of a uniform network architecture approach are that interoperable, and upgradeable networks can be built at lowest possible cost, because development has already been done in the commercial world. In addition it is faster to field operational capability because the components already exist, and future proofing is possible to a greater extent, since commercial pressures exist to develop long lifetimes. However legacy systems will remain an important issue for the foreseeable future.

The Defence Intranet Architecture described here has much in common with the INSC programme. It extends the INSC principles by practical incorporation of legacy C2 systems, a vital part of battlefield communications assets.

The proposed architecture offers three key benefits:

- Maintenance of robust secure legacy assets as the core national C2 capability,

- Provision of high-bandwidth, flexible-information architectures to enable information gathering from a diverse set of ISTAR assets,
- Facilitation of interoperability between coalition partners through an 'open' Internet architecture.

In addition to describing the architecture this paper has presented work which is focussed on addressing some of the issues:

- Information management will remain a key application requiring information management tools, enabling a range of novel applications, such as BATCOM,
- Security needs are paramount in military contexts, but are not inherently dissimilar to commercial needs for which currently acceptable solutions now exist,
- IP/VPN subnets lead to header inefficiency, as identified in INSC, but this can be overcome by header compression techniques
- Trust will increasingly be a vital part of a coalition network based on Internet concepts but models are being produced as exemplified by the MIND project.

Despite reservations about the robustness of commercial communications systems for military use, recent conflicts have in fact shown increased use of commercial technology. The defence intranet architecture proposed here offers a framework for the systematic inclusion of COTS assets into the battlespace in preference to the current more ad-hoc arrangement. Moreover the architecture will, it is argued, ease interoperability among NATO partners issues making alliances more effective in the future.

REFERENCES

[1] Network Centric Warfare. Alberts, Garstka, and Stein. (1999) http://www.dodccrp.org/research/ncw/ncw.htm

[2] NEC Outline Concept: Executive Summary Dstl/IMD/SOS/500/2, Issue 2.0, 2 May 2003 http://www.mod.uk/issues/nec/concept_papers.htm

[3] Architectural Principles of the Internet. B. Carpenter, Ed., IETF RFC 1958, June 1996.

[4] A Goal Architecture for Network Enabled Capability, B.J. Sowerbutts and R. Sharman, RMR white paper, 2003

[5] Header and Signalling Compression in Military IP networks, A. Surtees, R. Price, M. West, R. Hancock, P. Ollis, S. McCann, in InterOperable Networks for Secure Communications Symposium, Hague, 2003.

[6] Improved TCP Performance over Long-delay and Error-prone Links, M. West, S. McCann, IEE Seminar on Satellite Services and the Internet, 2000.

[7] Ad Hoc Meshes in IP based Military Networks, R. Hancock, M. West, E. Hepworth, B.J. Sowerbutts, in InterOperable Networks for Secure Communications Symposium, Hague, 2003.

[8] Interoperable Networks for Secure Communications http://insc.nodeca.mil.no/ifs/files/startframe.html

[9] Swarming, Network Enabled C4ISR Conference, UNCLASSIFIED, 13-14 January 2003, McLean, VA.

[10] Future Combat Systems, J Schmidt, (FCS Lead Systems Integrator Program Director for Force Requirements) - USA, Swarming Network Enabled C4ISR Conference, UNCLASSIFIED, 13-14 January 2003.

[11] Flexible Security, P. Davies, Thales White paper on Cryptography and Interoperability, http://www.thales-esecurity.com/Whitepapers/wpNetwork_Security.shtml

[12] MIND protocols and mechanisms specification, simulation and validation, IST Project MIND Deliverable 1.2 November 2002.

Evolving Interoperable Network Architectures for NATO Coalition Forces

Barry Sowerbutts, Richard Sharman, Mark West
Roke Manor Research Ltd
Roke Manor, ROMSEY
Hants, UK, SO51 0ZN
barry.sowerbutts@roke.co.uk

Roke Manor Research

- A technical consultancy, providing custom solutions in communications and sensor systems
- Full design life-cycle: new design, modification or add-on
- 350+ professional engineers: state-of-the-art skills in all ‘hard’ and ‘soft’ technologies
- Purpose-built laboratories, all design & prototyping facilities on site. ISO 9001 and TickIT quality accreditation. Full UK Govt. List X status.
- 40+ year pedigree – owned by Siemens since 1991, but operates independently
- Wide customer base: Siemens, HM Govt., many commercial organisations
- Turnover approx €45m

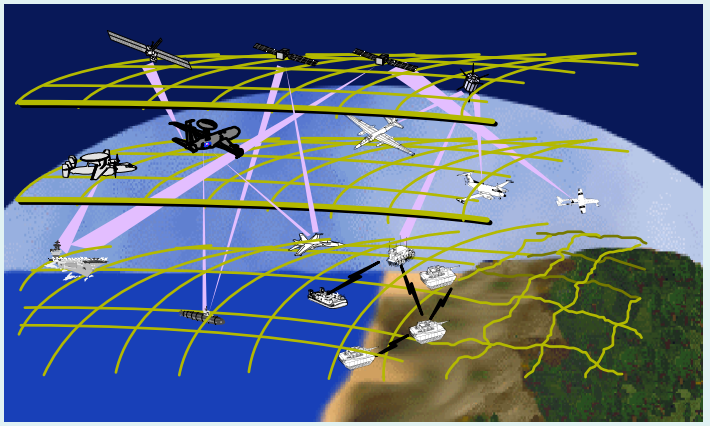
Evolving Network Architectures

Roke Manor Research

- Network Enabled Capability and the rationale for a new architecture
- A description of the proposed architecture and applicability to coalition operations
- A testbed as an element of the architecture
- Some issues
- Conclusions and next steps

Network Enabled Capability Themes

- Themes
  - Full information availability
  - Shared awareness
  - Flexible working
  - Agile mission groups
  - Synchronised effects
  - Effects-based planning
  - Resilient information infrastructure
  - Fully networked support



The Need for an Architecture

- Network Enabled Capability
  - Predicated on achieving new levels of
    - Capacity
    - Interoperability
  - Needs advanced network architectures
    - A major motivation for this work
    - Recognising significant advances made in the civil world using IP
      - Separating bearer from application
      - Rapid application evolution and sharing
      - Rapid bearer evolution and diversification

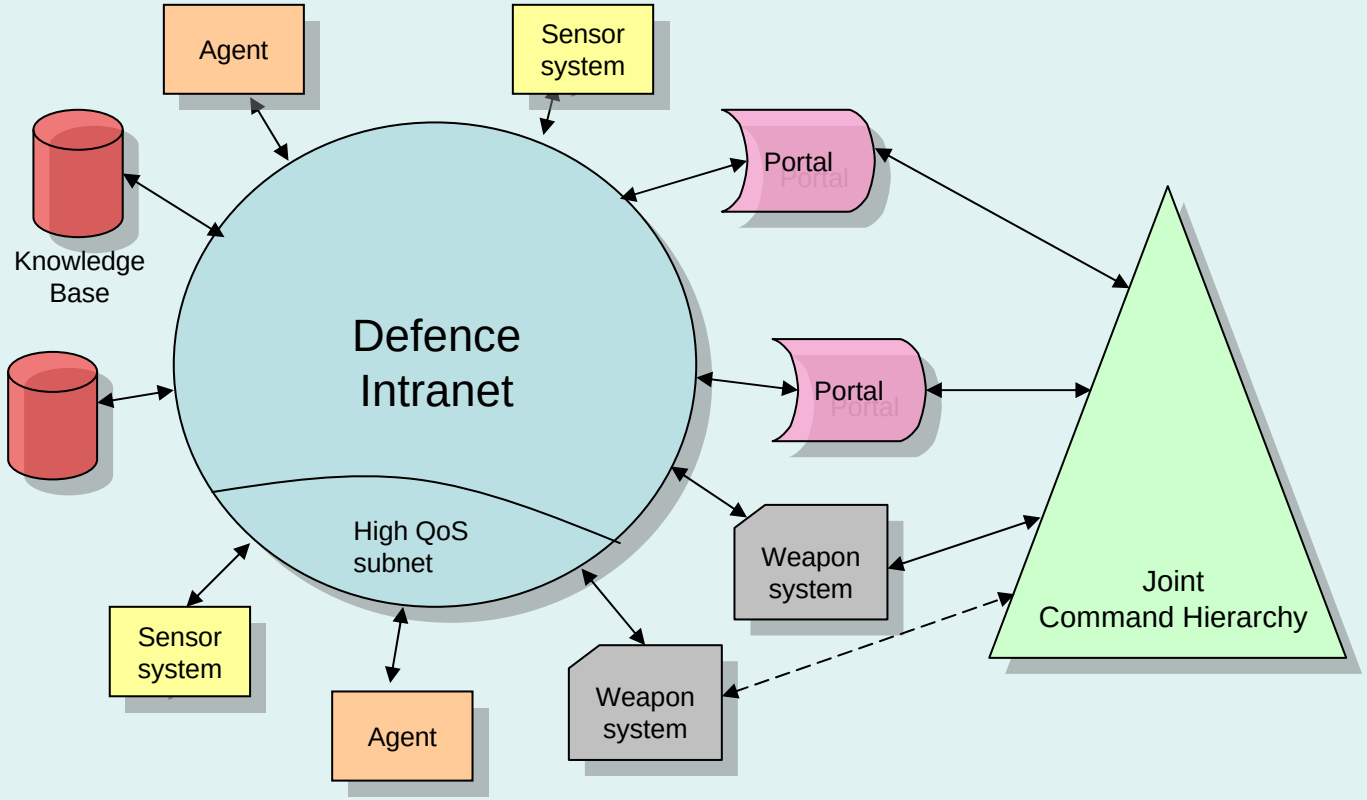
Starting from here

- Legacy Systems
  - Requirements
    - Robustness, Security, Specific Function
  - But Limited …
    - Bandwidth, interoperability, adaptability
- Future Legacy
  - Improved performance
  - Internet-like features internally
  - But lacking architectural flexibility

Constraints

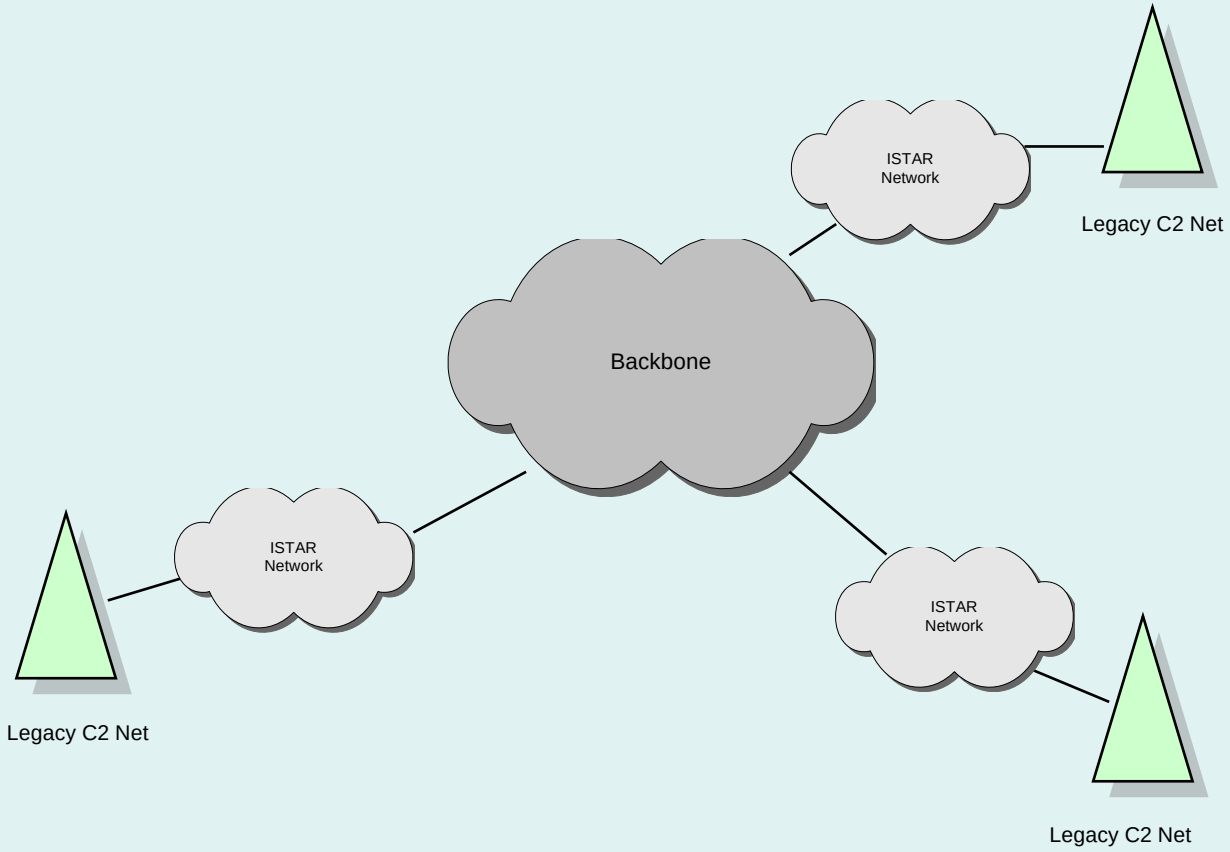
- C2 functions essential
  - Highly-robust and secure communications
- Significantly increased ISTAR requirements
  - High bandwidth information capture and dissemination
- Addressing, Routing, Discovery, Confign
  - Will stress military equipment in terms of flexibility
- Flexible capacity acquisition
  - Service-based acquisition
- Application innovation
  - Transparency of application interface
- Security
  - Broader interpretation

The Defence Intranet Architecture



Evolution of the Architecture to support Coalition Operations

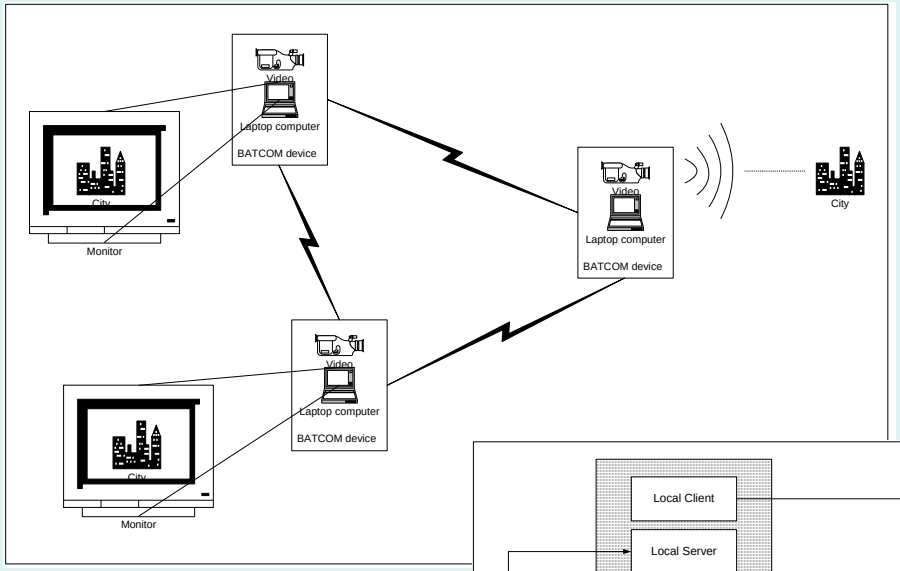
Roke Manor Research

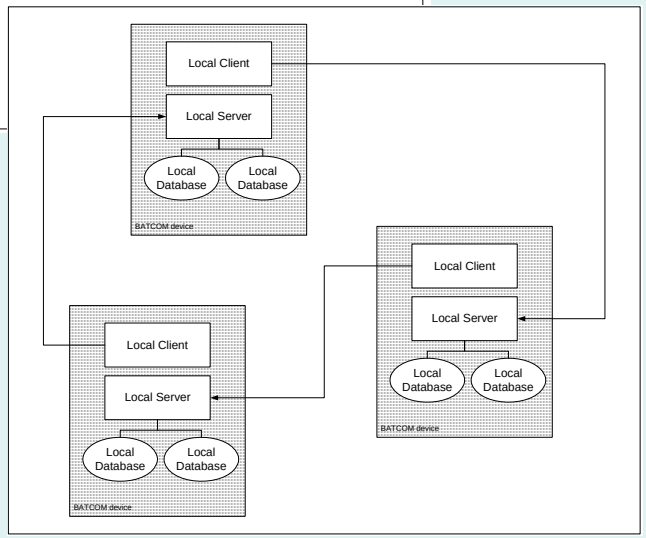


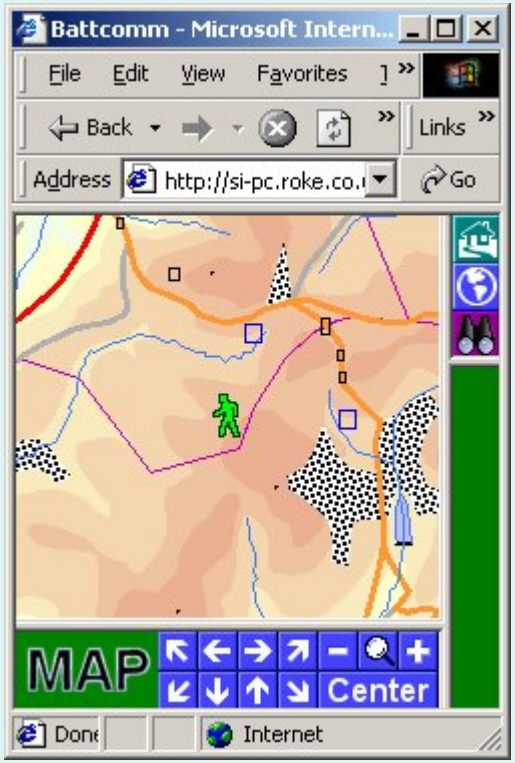
Steps in the Evolution

- Address space definition
- Routing policy selection
- Management policy selection
- Legacy interconnection
- Application growth

A Testbed





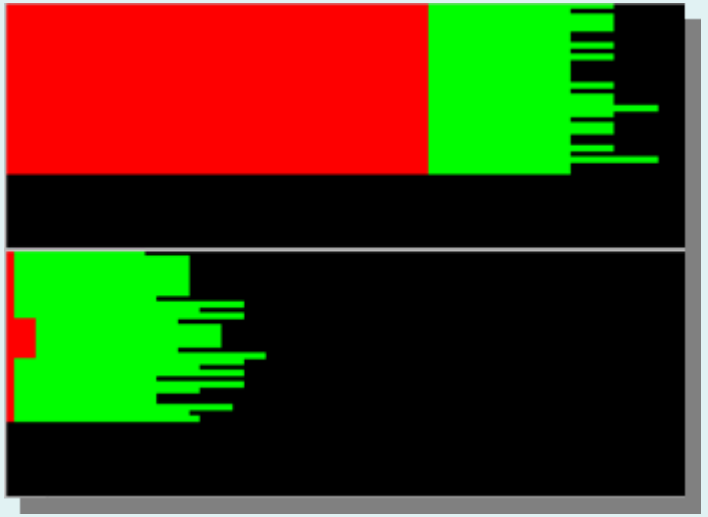


Issues

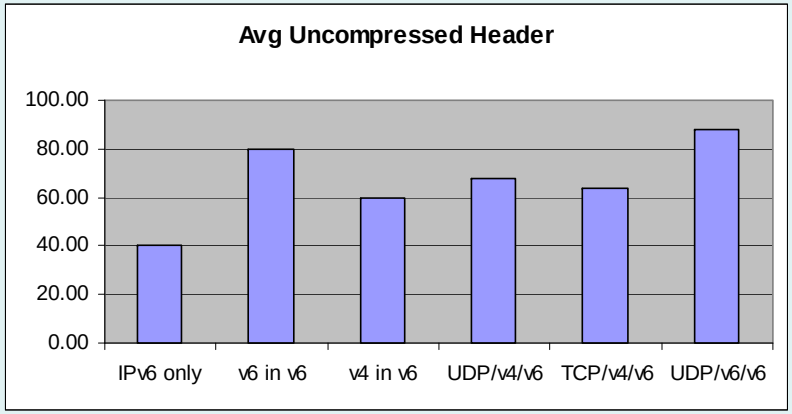
- IPv4-v6 transition
  - Multilayer networks
  - IPSEC tunnels
  - Concatenated headers
  - Experienced in INSC
- Trust in coalition networks
  - Shared use of resources
  - Trust model
  - Research in EU IST 5th Framework

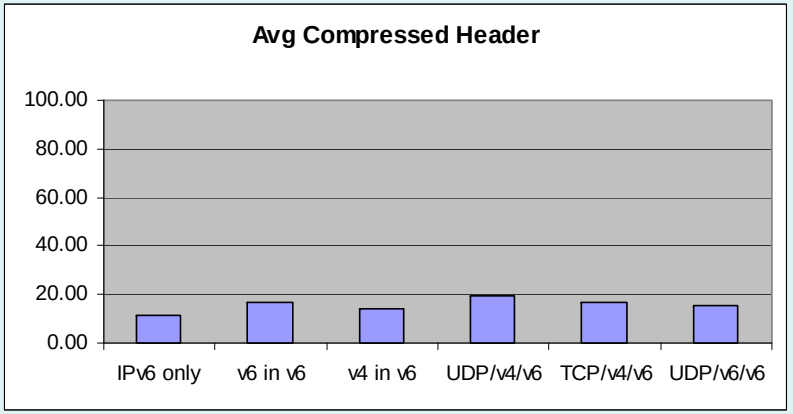
The need for Header Compression

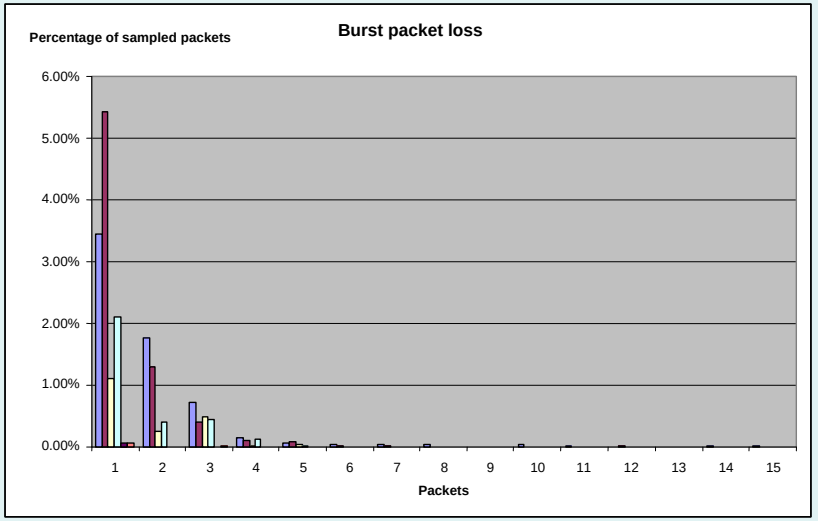
- Robust Header Compression
  - Dramatically reduces packet overhead over the air
  - Provide a valuable increase in utilisation
  - Highly resilient to packet loss in the presence of bit errors
  - Being standardised in IETF
  - Software successfully trialled by RMR in INSC



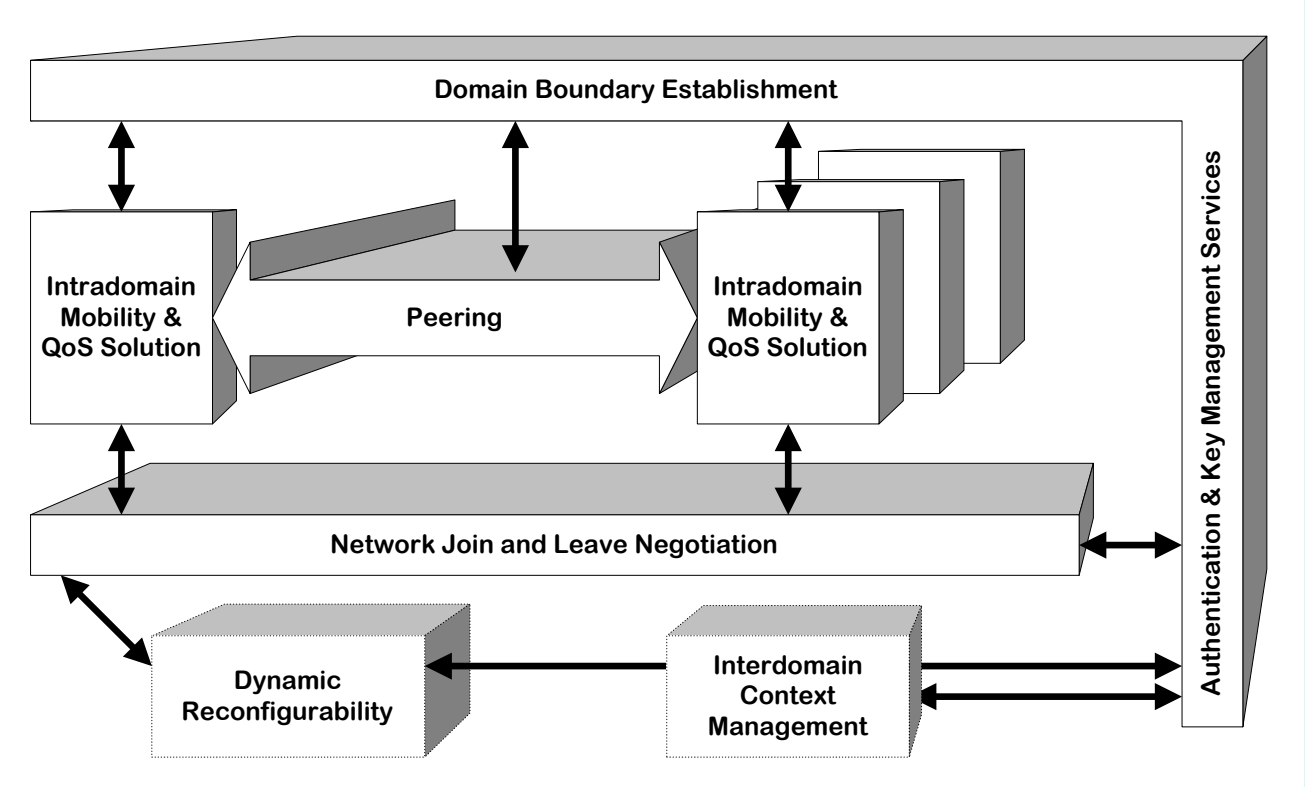
Header Compression Results







Trust in the Coalition Network



Conclusions

- Network Enabled Capability will enable flexible and rapid force deployment
- *But …*
- Progress is predicated on enhanced capacity and interoperability requirements
- *Needing …*
- Advanced architectural solutions

Conclusions

- A novel architecture has been described which
  - Maintains robust secure legacy assets as the core national C2 capability,
  - Provides high-bandwidth, flexible-information architectures to enable information gathering from a diverse set of ISTAR and other assets,
  - Facilitates interoperability between coalition partners through an ‘open’ Internet architecture.
- Information management will remain a key requirement enabled by a range of novel applications, an example of which has been presented

Conclusions

- Some issues for coalition working
  - IP/VPN subnets lead to header inefficiency, as identified in INSC, but this can be overcome by header compression techniques and results have been presented here
  - Trust will increasingly be a vital part of a coalition network based on Internet concepts, but models are being produced as exemplified by the IST MIND project and summarised here.
- Next steps
  - Modelling information exchange requirements
  - Analysing trust issues in the coalition architecture